Westlaw Today
powered by Reuters

Mandatory breach notification requirements for government contractors are almost here

By Leah Kaiser, Esq., Husch Blackwell LLP*

JULY 9, 2021

President Biden's newly released Executive Order on Improving the Nation's Cybersecurity[1] represents a comprehensive approach to tackling cybersecurity threats in the U.S. and will likely result in new FAR and DFARS contract requirements.

Currently, breach notification requirements in government contracts are a patchwork affair depending on the contracting agency and the type of information involved.

It represents the next step towards the inclusion of mandatory breach notifications in government contracts following widespread speculation that breach notification requirements were on the horizon.[2]

The EO mirrors the recent national interest in cybersecurity that has dominated multiple sectors[3] and that has grown in response to recent cybersecurity attacks that have captured national attention, such as the Colonial Pipeline incident.

The EO declares "the prevention, detection, assessment, and remediation of cyber security incidents" as a top priority and appears to focus on breach notifications as a key component. Currently, breach notification requirements in government contracts are a patchwork affair depending on the contracting agency and the type of information involved.

The EO calls for the Director of the Office of Management and Budget (OMB) in consultation with other parties to review the FAR and DFARS to ensure that IT and OT service providers:

- Collect, preserve, and report data and information relating to the preventing, detection, and response to cybersecurity events
- Share this information with "any agency with which they have contracted, directly with such agency and any other agency that the Director of OMB, in consultation with the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence, deems appropriate, consistent with applicable privacy laws, regulations, and policies"
- Collaborate with Federal cybersecurity or investigative agencies in responding to and investigating occurring and threatened incidents
- Share information in industry-recognized formats when possible to further collaboration

Additionally, the EO directs the Secretary of Homeland Security in conjunction with a number of other parties to recommend contract language to the FAR Council that identifies the types of cyber incidents that must be reported and the associated information, civil liberty and privacy protections, time periods for reporting based on severity, National Security Systems reporting requirements, and the kind of contractors and service providers to be subject to the proposed language.

Finally, the EO contains provision regarding agency use of cloud technology, software supply chain security, the establishment of a new Cyber Safety Review Board, and a focus on standardizing the response and identification of cybersecurity vulnerabilities and incidents.

The EO directs the Secretary of Homeland Security in conjunction with a number of other parties to recommend contract language to the FAR Council that identifies the types of cyber incidents that must be reported.

Ultimately, the FAR Council will review the recommendations and the proposed contract language generated by the EO and, as appropriate, will publish the proposed updates for public comment.

Contractors should, if they haven't already, begin to develop internal systems for identifying and reporting cybersecurity threats so that they can easily assimilate if and when new FAR provisions are published. Furthermore, contractors who have concerns about sharing this information should plan to voice those during the public comment period.

Notes

[1] https://bit.ly/3ysQaMu

[2] https://bit.ly/2Uw8mFo

[3] https://bit.ly/3jTcZEc

About the author

Leah Kaiser is an attorney in **Husch Blackwell LLP**'s Washington, D.C., office. She can be reached at leah.kaiser@huschblackwell.com. This article was originally published June 23, 2021, on the firm's website. Republished with permission.

This article was first published on Westlaw Today on July 9, 2021.